# EXHIBIT A

# UNITED STATES DISTRICT COURT

for the

Western District of Washington



In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*
The property and person more fully described in Attachments A-1 and A-2.

Case No: MJ21-287

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachments A-1 through A-2, which are incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachments B-1 and B-2, which are incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 21 U.S.C. 841 (a)(1), 21 U.S.C. 846 | distribution of controlled substances, conspiracy to do the same |

The application is based on these facts:

✓ See Affidavit of United States Postal Inspector Michael Fischlin continued on the attached sheet.

☐ Delayed notice of ____ days (give exact ending date if more than 30 days: ____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

[signature]
*Applicant's signature*

Michael Fischlin, U.S. Postal Inspector
*Printed name and title*

○ The foregoing affidavit was sworn to before me and signed in my presence, or
◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 05/14/2021

[signature]
*Judge's signature*

City and state: Bellingham, Washington

Paula L. McCandlis, United States Magistrate Judge
*Printed name and title*



USAO 2021R00505

# AFFIDAVIT OF MICHAEL FISCHLIN

STATE OF WASHINGTON )
) ss
COUNTY OF KING )

I, Michael Fischlin, an Inspector with United States Postal Inspection Service ("USPIS"), Seattle, Washington, having been duly sworn state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I am a Postal Inspector with the USPIS and have been so employed since June 2016. I am an "investigative or law enforcement officer of the United States" within the meaning of Title 18, United States Code, Section 2510(7). I am currently assigned to the Seattle Division, Contraband Interdiction & Investigations Team, where I investigate the use of the United States Postal Service ("USPS") to transport controlled substances, the proceeds of drug trafficking, and instrumentalities associated with drug trafficking. I have received specialized training in the investigation of controlled substances in the United States mails. I have also received training on the identification of controlled substances, interdiction of controlled substances and proceeds thereof.

2. Prior to becoming a Postal Inspector, I was employed as a Special Agent ("SA") of the United States Secret Service ("USSS"). As part of my training, I completed the Federal Law Enforcement Training Center Criminal Investigator Training Program as well as the USSS SA Training Program. While employed by the USSS, I was trained in computer forensics. Prior to joining the USSS, I served four years of active duty in the United States Marine Corps as a military policeman.

3. As a Postal Inspector, I am authorized to investigate crimes involving federal offenses relating to the USPS. During the tenure of my law enforcement career, I have been involved in a wide spectrum of investigations, which include access device fraud, bank fraud, computer fraud, controlled substances, counterfeit currency and securities, identity theft, mail theft, robbery, threats, and wire fraud. My duties have



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

included planning the execution of search warrants; securing and searching premises; seizing documents, records and other evidence; and interviewing witnesses.

4. The information in this affidavit is based upon the investigation that I have conducted in this case, my conversations with other law enforcement officers who have engaged in various aspects of this investigation, and my review of reports written by other law enforcement officers involved in this investigation. Because this Affidavit is being submitted for the limited purpose of securing search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are relevant to a determination of probable cause to support the issuance of the requested warrants. When the statements of others are set forth in this Affidavit, they are set forth in substance and in part.

## PURPOSE OF AFFIDAVIT

5. This affidavit is submitted in support of an application for search warrants for the following location and person:

(1) 27340 Village Pl NW, Stanwood, WA 98292 (the "SUBJECT PREMISES"), further described in Attachment A-1, which is incorporated herein by reference; and

(2) The person of Christopher FRICK (AKA Christerfer Frick), further described in Attachment A-2, which is incorporated by reference.[1]

6. For the SUBJECT PREMISES, the requested authority to search extends to all parts of the property, including all storage areas associated with the residence, such as on-site storage lockers or safes located on the property, whether locked or not, where the items described in Attachment B-1, (list of items to be seized) could reasonably be found.

7. As set forth below, there is probable cause to believe that the SUBJECT PREMISES and FRICK will contain or possess evidence of possession of controlled substances with intent to distribute, distribution of controlled substances, and conspiracy

[1] The spelling of FRICK's first name on his Washington State driver license is spelled *Christerfer*.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

to do the same, in violation of Title 21, United States Code, Sections 841(a) and (b), as well as Section 846. I seek authorization to search and seize the items specified in Attachments B, which are incorporated herein by reference.

## BACKGROUND ON THE DARK WEB

8. The "dark web" is a portion of the "Deep Web" of the Internet, where individuals must use anonymizing software or applications to access content and websites. Within the dark web, criminal marketplaces operate, allowing individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes called the "clear web" or simply the "web"). These online market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring. Famous dark web marketplaces, also called Hidden Services, such as Silk Road, operated similarly to clear web commercial websites such as Amazon and eBay, but offered illicit goods and services. Other dark web markets described herein – including Dark0de Market and White House Market – operate similarly. There are numerous marketplaces that have appeared on the dark web that have offered contraband for sale, including narcotics. Users typically purchase narcotics through these marketplaces using digital currency such as bitcoins.

9. "Vendors" are the dark web's sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of "vendor accounts" on dark web marketplaces. Customers, meanwhile, operate "customer accounts." Vendor and customer accounts are not identified by numbers, but rather monikers or "handles," much like the username one would use on a clear web site. If a moniker on a particular marketplace has not already been registered by another user, vendors and customers can use the same moniker across multiple marketplaces. Based on customer reviews, vendors can become well known as "trusted" vendors.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

10. It is also possible for the same person to operate multiple customer accounts and/or vendor accounts at the same time. For example, based on my training and experience, I know that one person could have a vendor account that he or she uses to sell illegal goods on a dark web marketplace in exchange for cryptocurrency; that same vendor could also have a different customer account that he or she uses to purchase illegal goods from other vendors. Because they are separate accounts, a person could use different accounts to send and receive the same cryptocurrency on the dark web. I know from training and experience that one of the reasons dark web vendors have multiple monikers for different vendor and customer accounts is to prevent law enforcement from identifying which accounts belong to the same person and who the actual person is that owns or uses the accounts.

11. Pretty Good Privacy ("PGP") is used on dark web markets to encrypt communications between vendors and customers. When a customer orders from a vendor or sends a vendor a message on a dark web market, that information may be stored in the marketplace's database. The marketplace server may be hacked or seized by law enforcement, and a customer may not want their private messages with any sensitive information, like name and address, easily viewable by anyone who obtains access to the database. These messages may also be seen by someone who has access to the vendor's computer or market account, such as a market administrator. PGP encryption is used to solve this problem.

12. A vendor has both a PGP private key and a public key. A customer can use the vendor's public key to encrypt a message. The vendor then uses their private key to decrypt the message. Vendors keep their private key secure but not their public key, which they put on their profile. This is done so customers may use a vendor's PGP public key to encrypt data sent to the vendor, such as the customer's name and address. Only the corresponding PGP private key, held by the vendor, can decrypt the data.

13. When registering an account on a dark web marketplace, users are often provided with a mnemonic phrase. A mnemonic phrase is a list of random words which



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

allow a user to access their account if the password is lost or forgotten. If a password is lost or forgotten, a user will be asked to provide their mnemonic and login username to reset the password. Dark web marketplaces only display the page containing a user's mnemonic phrase once after an account is created. Markets recommend that the mnemonic be stored in a safe location.

14. The Onion Router or "Tor" network is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and thereby the locations and identities of the network's users. Tor likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such "hidden services" operating on Tor have complex web addresses, which are many times generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software designed to access the Tor network. Most "hidden services" are considered dark web services with no legitimate or identified service provider to which legal process may be served.

## BACKGROUND ON CRYPTOCURRENCY

15. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies.[2] Examples of cryptocurrency are Bitcoin[3] ("BTC"), Litecoin ("LTC"), and Monero ("XMR"). Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency

[2] Fiat currency is currency created and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.
[3] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) or "BTC" to label units of the cryptocurrency. That practice is adopted here.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[4] Cryptocurrency is not illegal in the United States.

16. Bitcoin is a type of digital currency. Payments or transfers of value made with bitcoins are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoins through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), Bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" bitcoins by using his/her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smartphones.

17. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as "pseudonymous," meaning that they are partially

[4] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

anonymous. And while it is not completely anonymous, Bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and credit systems.

18. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key (or public address) is akin to a bank account number, and a private key (or private address) is akin to a Personal Identification Number ("PIN") number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public key and the private key. A public address is represented as a case-sensitive string of letters and numbers. Each public address is controlled and/or accessed through the use of a unique corresponding private key—the cryptographic equivalent of a password or PIN—needed to access the address. Only the holder of an address's private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

19. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including: on a tangible, external device ("hardware wallet"); downloaded on a Personal Computer ("PC") or laptop ("desktop wallet"); with an Internet-based cloud storage provider ("online wallet"); as a mobile application on a smartphone or tablet ("mobile wallet"); as printed public and private keys ("paper wallet"); and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smartphones or tablets) or at websites that users can access via a computer, smartphone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a Universal Serial Bus ("USB") thumb drive or other commercially available device designed to store cryptocurrency (e.g. Keepkey, Nano Ledger, or Trezor). In addition, paper wallets may



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

contain an address and a QR code with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

20. Although cryptocurrencies such as Bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering, and is an oft-used means of payment for illegal goods and services on hidden services websites operating on the Tor network. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplaces. As of May 12, 2021, one bitcoin is worth approximately $54,140, though the value of Bitcoin is generally much more volatile than that of fiat currencies.

## SUMMARY OF INVESTIGATION

### A. Subject Moniker, Controlled Buys, and Seized Parcels

21. On April 15, 2021, an undercover federal agent placed an order for synthetic heroin from the Subject Moniker on Dark0de Market, a dark web marketplace.[5] The method of payment was XMR.[6] Law enforcement subsequently received a parcel containing a white powdery substance. Analysis by the USPS Forensic Laboratory indicated that the substance contained fentanyl and heroin.[7] USPS business records

[5] Investigators wish not to reveal the moniker at this time as keeping it confidential may have investigative value.
[6] Monero, which is abbreviated to "XMR," is a cryptocurrency focused on privacy. Transactions on the Monero blockchain are obscured making its users more difficult to track or trace.
[7] Fentanyl is a Schedule II controlled substance. Heroin is a Schedule I controlled substance.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

showed that the parcel was first scanned in Granite Falls, Washington. The parcel bore a pre-printed USPS shipping label purchased from a third-party vendor. In addition, the listed sender was a business located in Seattle, Washington.

22. On April 19, 2021, I spoke with a USPS employee at the Granite Falls Post Office ("PO"). The employee believed the parcel had been deposited into the USPS blue collection box outside of the PO.[8] The employee recalled collecting several such parcels which she found odd for several reasons including that they displayed a Seattle sender address yet were mailed from Granite Falls, Washington.

23. On April 22, 2021, I placed an order for heroin from the Subject Moniker on White House Market, a dark web marketplace. The method of payment was XMR. I subsequently received a parcel containing a tan powdery substance. Analysis by the USPS Forensic Laboratory indicated that the substance contained fentanyl and heroin. USPS business records showed that the parcel was first scanned in Arlington, Washington. The parcel bore a pre-printed USPS shipping label purchased from a third-party vendor. In addition, the listed sender was a business located in Seattle, Washington.

24. On April 24, 2021, I was contacted by a USPS employee from the Granite Falls PO. The employee advised that she had found three parcels in the mail receptacle located within the lobby of the PO with labels similar to the parcel law enforcement received from the Subject Moniker. The parcels are flat rate envelopes and no other flat rate envelopes were found in the mail receptacle. A federal search warrant was executed for one of the parcels (hereafter the "seized parcel") which contained blue pills imprinted "M" on one side and "30".[9] One random pill was analyzed by the USPS Forensic Laboratory which indicated that the pill contained fentanyl. The intended recipient was

---

[8] A collection box is a blue box which provides a reliable, secure, and convenient receptacle for people to deposit outgoing mail.

[9] It should be noted the Subject Moniker offers M30 oxycodone pills for sale on the dark web.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

later interviewed and advised he had ordered drugs from Subject Moniker 2 on Vice City, a dark web marketplace.[10]

25. Security footage from the Granite Falls PO showed that on the early morning of April 24, 2021, a male entered the PO and deposited three parcels, which appeared to be flat rate envelopes, into the mail receptacle located within the lobby. Flat rate envelopes measure approximately 12.5" x 9.5" which are significantly larger than letter size envelopes. The individual subsequently used a key to open a PO Box (hereafter "Edwards' PO Box") before departing the premises. The application for Edwards' PO Box revealed Edwards was the applicant. Furthermore, USPS business records revealed Edwards had submitted a change of address to Edwards' PO Box in March 2021. The male seen in security footage resembled Edwards' Washington State driver license photograph.

26. On April 29, 2021, I was contacted by an USPS employee from the Granite Falls PO. At approximately 5:39 am, the employee had found nine parcels in the mail receptacle located within the lobby of the PO with labels similar to the label on the seized parcel. The parcels are flat rate envelopes and no other flat rate envelopes were found in the mail receptacle. A federal search warrant was executed for those parcels which contained pills imprinted "M" on one side and "30", a tan powdery substance, and white powdery substances.[11] The suspected controlled substances within those parcels were concealed in the same manner as the substances found within the seized parcel and the parcels received by law enforcement from the Subject Moniker. This included the use of distinctive tape to secure the inner packaging. It should be noted that the Subject Moniker's advertisements for heroin include photographs of both tan and white

[10] Investigators wish not to reveal the moniker at this time as keeping it confidential may have investigative value.

[11] Some of the pills presumptively tested positive for the presence of Tramadol, a Schedule IV controlled substance. The powder substances were field tested with inconclusive results. The substances will need to be sent to a laboratory for analysis.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

substances; and that the Subject's Moniker offers oxycodone for sale which is known to be imprinted "M" on one side and "30" on the other.

27. Security footage from the Granite Falls PO showed that on April 28, 2021, at approximately 11:26 pm, a male entered the PO and deposited numerous parcels, which appeared to be flat rate envelopes, into the mail receptacle located within the lobby. The individual subsequently used a key to open Edwards' PO Box before departing the premises. The male seen in security footage resembled Edwards' Washington State driver license photograph.

28. On April 29, 2021, I placed an order for oxycodone pills from the Subject Moniker on Dark0de Market. The method of payment was BTC. To date, nothing has been received.

29. On May 4, 2021, I viewed the Subject Moniker's profile on Dark0de Market. Dark0de Market showed that the Subject Moniker had conducted 197 sales with a 4.74/5 rating. The Subject Moniker's profile advertised listings for heroin, methamphetamine, and oxycodone. The Subject Moniker's sales were calculated, which revealed approximately 251 grams of heroin had been sold on Dark0de Market.[12]

30. I also viewed the Subject Moniker's profile on White House Market. White House Market showed that the Subject Moniker had conducted 240 to 250 sales with 92% positive feedback. The Subject Moniker's profile advertised listings for heroin and oxycodone. The Subject Moniker's sales were calculated, which revealed approximately 355 grams of heroin had been sold on White House Market.[13] Feedback left by several customers indicated that the Subject Moniker's products were potent and had led to overdoses.

31. On May 6, 2021, I was contacted by an USPS employee from the Granite Falls PO. The employee advised that she had found ten parcels in the mail receptacle

[12] The Subject Moniker's sales consisted of a combination of both natural and synthetic heroin.
[13] The Subject Moniker's sales consisted of a combination of both natural and synthetic heroin.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

located within the lobby of the PO with labels similar to the labels on previously seized parcels. The parcels were flat rate envelopes and no other flat rate envelopes were found in the mail receptacle. A federal search warrant was executed for those parcels which contained pills imprinted "M" on one side and "30" on the other, tan powdery substances, and white powdery substances.

32. Security footage from the Granite Falls PO showed that on the evening of May 5, 2021, a male entered the PO and deposited numerous parcels, which appeared to be flat rate envelopes, into the mail receptacle located within the lobby. The individual subsequently used a key to open Edwards' PO Box and retrieve mail before departing the premises. The male seen in security footage resembled Edwards' Washington State driver license photograph.

**B. Search Warrant Execution and Interview**

33. On May 11, 2021, agents executed federal search warrants for Edwards' person, residence, and vehicle. Agents discovered on Edwards' person numerous pills imprinted "M" on one side and "30" on the other. Agents located the same type of pills in Edwards' residence as well as several empty parcels with labels similar to the labels on previously seized parcels.[14]

34. One of the parcels was addressed to the undercover name and address I provided to the Subject Moniker.[15] That package had been opened and there was nothing inside, corroborating Edwards' statement below that he would occasionally open and use drugs that FRICK gave him to mail. Four more opened and now empty packages that appeared to have been originally intended for mailing were located in Edwards' residence.

35. Federal agents interviewed Edwards at the Granite Falls Police Station after he provided his written consent and a waiver of his *Miranda* warnings.[16] Edwards stated

---

[14] The number of pills seized was user quantities – not distribution amounts.
[15] The parcel is believed to be associated with the undercover order referenced in paragraph 28 of this Affidavit.
[16] Edwards was involved in drug trafficking, used drugs, and the Court should assume that he had a drug problem.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

he mailed parcels for FRICK which Edwards knew contained drugs. Edwards knew this because he had opened some of the parcels received from FRICK and consumed the contents which consisted of powdery substances and M30 pills. Edwards retrieved parcels from FRICK at the SUBJECT PREMISES which were packaged and ready to be mailed.[17] FRICK told Edwards to place parcels into the mail stream outside of the city where the SUBJECT PREMISES is located. Edwards saw large quantities of powdery substances believed to be controlled substances at the SUBJECT PREMSIES. The powdery substances included a substance FRICK referred to as "china white".[18] Edwards also saw a vacuum sealer and white paper with information for where parcels should be sent in the garage of the SUBJECT PREMSIES. Edwards stated he had last mailed parcels for FRICK approximately one week ago. Edwards also indicated FRICK believed Edwards had recently been stealing parcels.

36. An agent showed Edwards a photograph of the Subject Moniker's profile picture on Dark0de Market. Edwards recognized the powdery substance in the photograph as what he had seen in parcels received from FRICK as well as what he had seen at the SUBJECT PREMISES.

37. Edwards said he had seen a variety of vehicles at the SUBJECT PREMISES to include an Audi sedan and a gold BMW Sport Utility Vehicle ("SUV").

38. I found an LG mobile phone in Edwards' vehicle.

39. Edwards stated both he and a person with the initials A.A. use the LG mobile phone recovered from his vehicle.[19] Edwards provided the PIN code to access the phone. Edwards advised FRICK's phone number was saved under the contact name of "Chris".

---

[17] Edwards showed a federal agent where the SUBJECT PREMISES is located on a map. Edwards also described the vehicles he had seen at the SUBJECT PREMISES.

[18] Some of the Subject Moniker's heroin listings on the dark web include china white in the product title.

[19] A.A. is Edwards' wife.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

40. During a review of Edwards' LG mobile phone, I found a text message sent to "Chris" on May 10, 2021. The message read, "So did you find out that i did put those in the mail for you and didn't steal them?" I also found communications on the LG mobile phone with "Chris Frick" via Facebook Messenger in April 2021.

41. It should be noted that records were received from T-Mobile for Edwards' phone number. Records showed that from March 29, 2021 to April 28, 2021, Edwards' phone number and the phone number saved under the contact "Chris" communicated approximately 300 times.[20]

42. According to court records, FRICK was sentenced to 108 months of federal imprisonment and five years of supervised release for Conspiracy to Distribute Controlled Substances in January 2013. FRICK is currently on supervised release.

**C. The SUBJECT PREMISES and Surveillance**

43. Open source research revealed the SUBJECT PREMISES was sold in November 2020 and the current taxpayer is a person with the initials J.S. Research further showed that a quit claim deed had been filed in FRICK's name on or about November 24, 2020, transferring interest in the SUBJECT PREMISES to J.S. Open source research showed that J.S. is FRICK's wife, and that the two married in November 2020.

44. On May 11, 2021, a federal agent conducted surveillance of the SUBJECT PREMISES. An agent observed an Audi sedan and a gold BMW SUV parked in front of the garage at the SUBJECT PREMISES matching the descriptions of vehicles provided by Edwards. Washington State Department of Licensing records showed that the gold BMW SUV is registered to J.S. at the SUBJECT PREMISES. There was no license plate on the back of the Audi sedan.[21]

---

[20] The communications consisted of a combination of phone calls and text messages.

[21] During Edwards' interview he stated FRICK had traded a Mazda RX-8 for an Audi sedan. Washington State Department of Licensing records showed FRICK owned a Mazda RX-8 with the SUBJECT PREMISES as his mailing address.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

45. On May 12, 2021, I contacted a USPS employee at the Stanwood PO. The employee advised FRICK receives mail at the SUBJECT PREMSIES. I also queried a law enforcement database which listed the SUBJECT PREMISES as FRICK's must recent address.

46. With the exception of the text messages between Edwards and FRICK, I have not made any prior efforts to obtain the evidence based on the consent of any party who may have authority to consent due to the nature of the evidence that I am attempting to obtain and the nature of the investigation. I believe, based upon the nature of the investigation and the information I have received, that if FRICK becomes aware of the investigation in advance of the execution of a search warrant, he may attempt to destroy any potential evidence, whether digital or non-digital, thereby hindering law enforcement agents from the furtherance of the criminal investigation.

**KNOWLEDGE BASED ON TRAINING AND EXPERIENCE**

47. Based upon my training and experience, and conversations with other experienced law enforcement agents and officers who have been involved in narcotics cases, I know the following:

48. The distribution of illegal narcotics is frequently a continuing activity lasting over months and years. Persons involved in the trafficking of illegal controlled substances typically will obtain and distribute controlled substances on a regular basis, much as a distributor of a legal commodity would purchase stock for sale. Similarly, such drug traffickers will maintain an "inventory," which will fluctuate in size depending upon the demand for and the available supply of the product.

49. Drug traffickers often keep records of their illegal activities not only during the period of their drug trafficking violations but also for a period of time extending beyond the time during which the trafficker actually possesses/controls illegal controlled substances. The records are kept in order to maintain contact with criminal associates for future transactions and so that the trafficker can have records of prior transactions for which the trafficker might still be owed money or might owe someone



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

else money. Dealers often keep these records in their homes and in vehicles that they own, use, or have access to.

50. It is common for drug dealers to conceal large quantities of currency, foreign currency, financial instruments, precious metals, jewelry, and other items of value which are proceeds from drug trafficking in their residences and in other storage areas associated with the residence, such as on-site storage lockers, garages, detached storage sheds, and parking stalls, or safes located on the property.

51. Evidence of excessive wealth beyond an individual's outward means is probative evidence of the distribution of controlled substances. Therefore, receipts showing the expenditure of large sums of money and/or the expensive assets are evidence of drug trafficking. Drug traffickers commonly keep the expensive assets themselves and/or documentation of the purchase of the asset (receipts, warranty cards, etc.) in their homes, places of business, and in vehicles that they own, use, or have access to.

52. It is common for drug dealers to maintain equipment and supplies (*i.e.*, scales, packaging, masking agents) on hand over a lengthy period of time, even when they do not have any controlled substances on hand. The aforementioned items are frequently maintained in the dealer's homes, places of business, stash houses or storage units, and in vehicles that they own, use, or have access to.

53. Based on my training and experience, drug dealers often have some amount of inventory – namely, illegal drugs – stored in their homes, places of business, stash houses or storage units, and in vehicles that they own, use, or have access to.

54. It is common for drug dealers to possess firearms and ammunition to protect their drugs, assets, and persons from hostile gangs, rival traffickers, other criminals, and from law enforcement. Persons who purchase and possess firearms also tend to maintain the firearms and ammunition for lengthy periods of time. Firearms can be acquired both legally and unlawfully, without official/traceable documentation. Persons who acquire firearms from Federal Firearms Licensees, through deliberate fraud and concealment, often will also acquire firearms from private parties and other sources



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

unknown to the Bureau of Alcohol, Tobacco, Firearms and Explosives. Persons who, whether legally or illegally, purchase, possess, sell and/or transfer firearms or ammunition commonly maintain the firearms or ammunition on their person, at their residence or business, or in a motor vehicle which they own and/or operate. Firearms or ammunition are often secreted at other locations within their residential curtilage, and the identification of these firearms will assist in establishing their origin. Persons who purchase, possess, sell and/or trade firearms or ammunition commonly maintain documents and items that are related to the purchase, ownership, possession, sale and/or transfer of firearms, ammunition, and/or firearm parts, including but not limited to driver's licenses, telephone records, telephone bills, address and telephone books, canceled checks, receipts, bank records and other financial documentation on the owner's person, at the owner's residence or business, or in vehicles that they own, use, or have access to. Additionally, these individuals often maintain holsters, spare magazines or speed loaders and other instruments to facilitate the use of firearms in furtherance of criminal activity or acts of violence.

55. It is common for members of drug trafficking organizations, in an attempt to disguise their identities and illegal activities, to use prepaid cellular telephones and prepaid long distance calling cards. Often the only way to connect a subject with a particular prepaid cellular telephone or calling card is to seize the phone or calling card from the trafficker or his residence. The aforementioned items are frequently maintained in the drug trafficker's residence, place of business, or other areas they have access to.

56. Drug dealers often carry many of the items described above – including (but not limited to) drugs, drug proceeds, firearms, cellular phones – on their person.

**USE OF DIGITAL DEVICES AND DARK WEB DRUG SALES**



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

57. As a result of my training and experience, I know that digital devices[22] must be used by individuals who engage in dark web drug sales. Suspects engaged in dark web drug sales use digital devices, such as computers and smartphones, and often transport those digital devices while conducting illegal activity. In particular, a suspect needs digital devices equipped with Tor software to access the Internet in order to navigate to the dark web marketplaces referenced in this Affidavit. Digital devices are further needed to establish a dark web persona; list contraband for sale; communicate with customers and associates on a dark web marketplace, through encrypted messages and other means; and to transfer digital currency to or from a marketplace to another wallet. As a result, one form in which these items may be found is as electronic evidence stored on a digital device.

58. I know that Tor software exists for both computers and smartphones that allow a user to access the dark web. For example, Tor Browser is freely available for download and allows for the use of Tor on computers. Tor Browser can also be run off a USB flash drive once inserted into a computer. In addition, Tor is available for Android phones by installing the package named Orbot. Orbot brings the features and functionality of Tor to the Android mobile operating system. Tor is also available for Apple iPhones by installing an app called Onion Browser.

59. While Tor is designed to protect a user's anonymity and privacy on the Internet, some artifacts may be recovered by a computer forensic examiner. Artifacts which may be found on a digital device equipped with Tor include the mere existence of

---

[22] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

a Tor application, as well as websites bookmarked by a user. While the installation of Tor in and of itself is not nefarious, the existence of the application would show a user had the ability to access the dark web. Furthermore, bookmarked websites would show sites a user visited.

60. Furthermore, I know that PGP applications exist for both computers and smartphones. PGP is often used to encrypt communication between individuals who operate on dark web markets. Forensic examination of digital devices may reveal the existence of PGP applications and keys. Extracted PGP keys may help investigators link a digital device and/or a suspect to a dark web identity.

61. As the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, *i.e.*, by saving an e mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmark" files. Digital information can also be retained unintentionally, e.g., traces of the path (including, but not limited to the IP address) of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. In other words, if a computer user were to go to the website called WWW.USDOJ.GOV, a "footprint" in the browser cache may be found pointing to that website, indicating that particular computer was used to visit that website. Therefore, a search of digital devices may lead to evidence that will assist me in identifying online storage accounts for which I may be able to obtain additional search warrants to locate further evidence in this case.

62. In addition, I know based on my training and experience that those engaged in dark web drug sales use digital devices to, for example: a) store PGP keys; b) store customer shipping information; c) store cryptocurrency wallets and information; d) store photographs of narcotics; and, d) purchase and print postage/shipping labels.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

63. In my experience dark web drug vendors often use digital devices such as smartphones to take photographs of drugs. Vendors then transfer the photographs to a computer, which is used to list their drugs for sale on a dark web marketplace. Furthermore, dark web drug vendors often use computers to type and print postage labels which are attached to parcels containing drugs shipped to customers. This is because typing both the sender and recipient information for labels on a smartphone is a tedious task, which is much easier using a computer with a keyboard. Computers rather than mobile phones are also used to create a vendor profile and listings on dark web marketplaces for a similar reason. Typing both profile information and product descriptions is tedious and easier done with a computer.

64. Based upon my training and experience, and conversations with other experienced law enforcement agents and officers who have been involved in narcotics cases, I know the following:

a. Drug dealers regularly use cell phones and other electronic communication devices to further their illegal activities. As a result, evidence of drug dealing can often be found in text messages, address books, call logs, photographs, emails, text messaging or picture messaging applications, videos, and other data that is stored on cell phones and other electronic communication devices. Additionally, the storage capacity of such devices allows them to be used for the electronic maintenance of ledgers, pay/owe logs, drug weights and amounts, customers contact information, not only during the period of their drug trafficking violations but also for a period of time extending beyond the time during which the trafficker actually possesses/controls illegal controlled substances. The records are kept in order to maintain contact with criminal associates for future transactions and so that the trafficker can have records of prior transactions for which the trafficker might still be owed money or might owe someone else money.

b. Drug traffickers increasingly use applications on smartphones that encrypt communications such as Wickr, or applications that automatically delete messages, such as Snapchat, in order to avoid law enforcement monitoring or recording of



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

communications regarding drug trafficking and/or money laundering. Evidence of the use of such applications can be obtained from smartphones and is evidence of a smartphone user's efforts to avoid law enforcement detection.

## SEARCH AND SEIZURE OF DIGITAL MEDIA

65. As described above and in Attachments B, this application seeks permission to search for items listed in Attachments B that might be found in the SUBJECT PREMISES or on FRICK'S person, including digital devices.

66. In order to examine digital media in a forensically sound manner, law enforcement personnel, with appropriate expertise, will conduct a forensic review of any digital media seized. The purpose of using specially trained computer forensic examiners to conduct the imaging of any digital media, or digital devices is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer forensic examiner, it is not always necessary to separate these duties. Computer forensic examiners and investigators often work closely with investigative personnel to assist investigators in their search for digital evidence. Computer forensic examiners are needed because they generally have technological expertise that investigative agents do not possess. Computer forensic examiners, however, may lack the factual and investigative expertise that an investigate agent may possess. Therefore, computer forensic examiners and investigative agents often work closely together. It is intended that the warrant will provide authority for the affiant to forensically review or seek the assistance of others in the USPIS or within other law enforcement agencies to assist in the forensic review of any digital devices.

67. I also know the following:

a. Based my knowledge, training, and experience, I know that computer files or remnants of such files may be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

cost. Even when files have been deleted, this information can sometimes be recovered months or years later with forensics tools. This is because when a person "deletes" a file on a computer, the data contained in the files does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in "swap" or "recovery" files.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what is has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Digital storage devices may also be large in capacity, but small in physical size. Because those who are in possession of such devices also tend to keep them on their persons, especially when they may contain evidence of a crime. Digital storage devices may be smaller than a postal stamp in size, and thus they may easily be hidden in a person's pocket.

68. As further described in Attachments B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

to believe that this forensic electronic evidence will be on digital devices found in the SUBJECT PREMISES or on FRICK's person, because:

a. Data on the digital storage medium or digital devices can provide evidence of a file that was once on the digital storage medium or digital devices but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to further establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g. registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search of "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

example, as described herein, computers typically contain information that log computer activity associated with user accounts and electronic storage media that connected with the computer. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit the crime (e.g. Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper content, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing a user's intent.

69. In most cases, a thorough search of a premises for information that might be stored on digital storage media or other digital devices often requires the seizure of the digital devices and digital storage media for later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic copy of the digital media's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

70. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is rarely possible to bring to the search site all the necessary technical manuals and specialized equipment necessary to consult with computer personnel who have expertise in the type of computer, operating system, or software application being searched.

71. The analysis of computer systems and storage media often relies on rigorous procedures designed to maintain the integrity of the evidence and to recover "hidden," mislabeled, deceptively named, erased, compressed, encrypted or password-protected data, while reducing the likelihood of inadvertent or intentional loss or modification of data. A controlled environment such as a laboratory, is typically required to conduct such an analysis properly.

72. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impracticable to search for data during the execution of the physical search of the premises. The hard drives commonly included in desktop and laptop computers are capable of storing millions of pages of text.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

73. A search of digital devices for evidence described in Attachments B may require a range of data analysis techniques. In some cases, agents may recover evidence with carefully targeted searches to locate evidence without requirement of a manual search through unrelated materials that may be commingled with criminal evidence. Agents may be able to execute a "keyword" search that searches through the files stored in a digital device for special terms that appear only in the materials covered by the warrant. Or, agents may be able to locate the materials covered by looking for a particular directory or name. However, in other cases, such techniques may not yield the evidence described in the warrant. Individuals may mislabel or hide files and directories; encode communications to avoid using keywords; attempt to delete files to evade detection; or take other steps designed to hide information from law enforcement searches for information.

74. Because several people share the SUBJECT PREMISES as a residence, it is possible that the SUBJECT PREMISES will contain digital devices or other electronic storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on those digital devices, this application seeks permission to search and if necessary to seize those digital devices as well. It may be impossible to determine, on scene, which digital devices contain the things described in this warrant.

75. The search procedure of any digital device seized may include the following on-site techniques to seize the evidence authorized in Attachments B:

a. On-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or co-conspirators.

b. On-site copying and analysis of volatile memory, which is usually lost if a computer is powered down, and may contain information about how the



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

computer is being used, by whom, when and may contain information about encryption, virtual machines, or steganography which will be lost if the computer is powered down.

c. On-site forensic imaging of any computers may be necessary for computers or devices that may be partially or fully encrypted in order to preserve unencrypted data that may, if not immediately imaged on-scene become encrypted and accordingly become unavailable for any examination.

## REQUEST FOR SEALING

76. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application, affidavit and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation and disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Disclosure of these materials would give the target of the investigation an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution.

## CONCLUSION

77. Based on the information set forth herein, there is probable cause to search the above described SUBJECT PREMISES, as further described in Attachment A-1, and the person of Christopher FRICK, as further described in Attachment A-2, for evidence, fruits and instrumentalities, as further described in Attachments B, of crimes committed by the individuals listed in this affidavit and their co-conspirators, specifically distribution of, and possession with intent to distribute, controlled substances, in violation of Title 21, United States Code, Section 841(a)(1) and (b).

MICHAEL FISCHLIN
United States Postal Inspector



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970